



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/600,547	06/20/2003	Masayuki Numao	JP920020102US1	6077

7590 12/04/2006

Louis P. Herzberg
Intellectual Property Law Dept.
IBM Corporation
P.O. Box 218
Yorktown Heights, NY 10598

EXAMINER

TOLENTINO, RODERICK

ART UNIT PAPER NUMBER

2134

DATE MAILED: 12/04/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/600,547	Applicant(s) NUMAO ET AL.	
	Examiner Roderick Tolentino	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 20 June 2003.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-25 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-25 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.


Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 20 June 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.


KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 04/19/2006
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. Claims 1 – 25 are pending.

Specification

2. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Claim Objections

3. Claim 10 is objected to because of the following informalities:

As per claim 10, the word 'secrete' is spelled improperly.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 2, 5, 11 – 19 and 22 – 25 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
6. As per claim 2, limitation recites "distributes said encrypted content without specifying said user terminal." It is indefinite as to how the sent information will get to a

Art Unit: 2134

receiver if a target isn't specified. For purposes of examination it will be interpreted to be the information encrypted is not restricted to a terminal that will be using it.

7. As per claims 11 – 18 and 22 – 25, the claims begin by directing the claim towards a type of invention even though each claim is dependent on a different type of invention. For example claim 11, states "A program for..." however, claim 11 is dependent on claim 4 which is directed towards a server. It is suggested that the claims be re-worded to be directed towards a single type of invention. For purposes of examination all claims will be read without their preambles.

8. As per claim 19, limitations recite variables 'k', 'n' and the equation $k(\leq n)$, it is indefinite as to how these relate to the keys and for purposes of examination will be interpreted to be keys in a distribution system.

9. Further in claims 5 and 19, limitation recites "oblivious transfer to generate." It is unclear as to what is oblivious and how it relates to generation. For purposes of examination it will be interpreted to be a transfer.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

11. Claims 1 – 25 are rejected under 35 U.S.C. 102(b) as being anticipated by Matsumoto U.S. Patent No. (6,215,877).

Art Unit: 2134

12. As per claims 1 and 20, Matsumoto discloses a key management server for managing secret keys and public keys corresponding to given attribute values; a user terminal for accessing said key management server to obtain attribute secret keys generated based on said secret keys, said attribute secret keys corresponding to attributes of said user terminal; and a provider terminal for generating an encrypted content that can be decrypted by said user terminal having said attribute secret keys corresponding to given attributes by means of said public keys (Matsumoto, Col. 2 Lines 60 – 67 and Col. 3 Lines 1 – 5), wherein said provider terminal distributes said encrypted content and said user terminal decrypts said encrypted content decryptable by means of said attribute secret keys of its own (Matsumoto, Col. 4 Lines 57 – 67).

13. As per claim 2, Matsumoto discloses provider terminal distributes said encrypted content without specifying said user terminal that is to receive said encrypted content (Matsumoto, Col. 6 Lines 39 – 59).

14. As per claim 3, Matsumoto discloses user terminal sends a set of attribute values indicating attributes of its own to said key management server; and said key management server generates said attribute secret keys unique to said user terminal based on, among said secret keys managed by said key management server, secret keys corresponding to the attribute values sent from said user terminal and sends said attribute secret keys to said user terminal (Matsumoto, Col. 4 Lines 37 – 49).

15. As per claim 4, Matsumoto discloses a key storage for storing secret keys and public keys corresponding to predetermined attribute values; an attribute secret key generator for obtaining a set of given attribute values and generating attribute secret

Art Unit: 2134

keys corresponding to said set of attribute values based on secret keys corresponding to said attribute values among said secret keys stored in said key storage (Matsumoto, Col. 2 Lines 60 – 67 and Col. 3 Lines 1 – 5), and a sending/receiving unit for receiving said set of attribute values from a given user terminal and sending said attribute secret keys generated by said attribute secret key generator to said user terminal (Matsumoto, Col. 4 Lines 57 – 67).

16. As per claim 5, Matsumoto discloses attribute secret key generator generates said attribute secret keys by using a protocol implementing oblivious transfer (Matsumoto, Col. 6 Lines 39 – 59).

17. As per claim 6, Matsumoto discloses a criteria key generator for obtaining public keys corresponding to attribute values indicating attributes of a recipient to which a content is to be sent and using said public keys to generate criteria keys that can be decrypted by secret keys corresponding to said public keys (Matsumoto, Col. 3 Lines 21 – 28), an encrypted content generator for encrypting said content based on said criteria keys (Matsumoto, Col. 9 Lines 45 – 65) and a sending unit for sending said encrypted content without specifying any recipient of said content via a network (Matsumoto, Col. 4 Lines 57 – 67).

18. As per claim 7, Matsumoto discloses criteria key generator combines, based on predetermined rules, criteria keys corresponding to the individual attribute values encrypted by using public keys corresponding to said individual attribute values to generate a criteria key for restricting recipients of said content (Matsumoto, Col. 4 Lines 37 – 49).

Art Unit: 2134

19. As per claim 8, Matsumoto disclose criteria key generator generates a session key for encrypting said content and a criteria key for decrypting said session key; and said encrypted content generator uses said session key to encrypt said content content (Matsumoto, Col. 4 Lines 37 – 49).

20. As per claim 9, Matsumoto discloses a sending/receiving unit for accessing a key management server managing secret keys and public keys corresponding to given attribute values to receive attribute secret keys corresponding to attributes established for said information processing apparatus, said attribute secret keys being generated based on said secret keys (Matsumoto, Col. 4 Lines 57 – 67) and a decryptor for obtaining an encrypted content and decrypting said content based on said attribute secret keys (Matsumoto, Col. 11 Lines 2 – 8).

21. As per claim 10, Matsumoto discloses sending/receiving unit sends a set of attribute values established for said information processing apparatus to said key management server and receives said attribute secret keys generated based on said set of attribute values from said key management server (Matsumoto, Col. 4 Lines 37 – 49).

22. As per claim 11, Matsumoto discloses a decryption key for decrypting information encrypted with a given public key (Matsumoto, Col. 9 Lines 25 – 43).

23. As per claim 12, Matsumoto discloses computer-implemented function of generating said attribute secret key generates said attribute secret keys by using a protocol implementing oblivious transfer (Matsumoto, Col. 4 Lines 37 – 49).

Art Unit: 2134

24. As per claim 13, Matsumoto discloses to encrypt and distribute a given content, causing said computer to implement the functions (Matsumoto, Col. 2 Lines 60 – 67 and Col. 3 Lines 1 – 5).

25. As per claim 14, Matsumoto discloses generating said criteria key combines, based on predetermined rules, criteria keys corresponding to the individual attribute values encrypted by using public keys corresponding to said individual attribute values to generate a criteria key for restricting recipients of said content (Matsumoto, Col. 4 Lines 37 – 49).

26. As per claim 15, Matsumoto discloses accessing a key management server managing secret keys and public keys corresponding to given attribute values to receive attribute secret keys corresponding to attributes established (Matsumoto, Col. 4 Lines 37 – 49) and attribute secret keys being generated based on said secret keys; and obtaining the encrypted content and decrypting said encrypted content based on the attribute secret keys (Matsumoto, Col. 2 Lines 60 – 67 and Col. 3 Lines 1 – 5).

27. As per claim 16, Matsumoto discloses generate decryption key for decrypting information encrypted with a given public key (Matsumoto, Col. 9 Lines 25 – 43).

28. As per claim 17, Matsumoto discloses to encrypt and distribute a given content (Matsumoto, Col. 2 Lines 60 – 67 and Col. 3 Lines 1 – 5).

29. As per claim 18, Matsumoto discloses content distributed over a network (Matsumoto, Col. 2 Lines 60 – 67 and Col. 3 Lines 1 – 5).

30. As per claim 19, Matsumoto discloses generating n secret keys and n public keys corresponding to said secret keys and storing said secret keys and public keys in a

Art Unit: 2134

given storage, obtaining information about k ($\leq n$) secret keys selected at random by a given client from among said n secret keys stored in said storage; reading said k secret keys corresponding to information about the obtained secret keys from said storage (Matsumoto, Col. 2 Lines 60 – 67 and Col. 3 Lines 1 – 5), and using a protocol for implementing oblivious transfer to generate decryption keys for decrypting information encrypted with said k public keys corresponding to the k secret keys and providing said generated decryption keys to said client (Matsumoto, Col. 4 Lines 57 – 67).

31. As per claim 21, Matsumoto discloses a key management server for managing secret keys and public keys for given attribute values; and a plurality of user terminals for accessing said key management server to obtain attribute secret keys corresponding to attributes of their own, said attribute secret keys being generated based on said secret keys (Matsumoto, Col. 2 Lines 60 – 67 and Col. 3 Lines 1 – 5), wherein a given one of said user terminals generates a group key and sends said group key to ones of the other user terminals and provides a content, said encrypted group key being decryptable by said ones of the other user terminals having said attribute secret keys corresponding to given attributes by means of said public keys, said content being only accessible by using said group key (Matsumoto, Col. 4 Lines 36 – 49).

32. As per claims 22 and 23, Matsumoto discloses key distribution (Matsumoto, Col. 2 Lines 60 – 67 and Col. 3 Lines 1 – 5).

33. As per claims 24 and 25, Matsumoto discloses computer usable medium (Matsumoto, Col. 15 Lines 5 – 15) and key distribution (Matsumoto, Col. 2 Lines 60 – 67

Art Unit: 2134

and Col. 3 Lines 1 – 5).

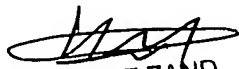
Conclusion

34. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Roderick Tolentino whose telephone number is (571) 272-2661. The examiner can normally be reached on 8:00am - 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.


Roderick Tolentino


KAMBIZ ZAND
PRIMARY EXAMINER

Roderick Tolentino
Examiner
Art Unit 2134